September 15, 2016

Network Penetration Reporting and Contracting for Cloud Services
(DFARS Case 2013-D018)
Frequently Asked Questions (FAQs) regarding the implementation of
DFARS Subpart 204.73 and PGI Subpart 204.73
DFARS Subpart 239.76 and PGI Subpart 239.76

http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html

The following questions are addressed in this document:

Q1: Why was the Network Penetration Reporting and Contracting for Cloud Services rule published as an interim rule?

A1: A determination was made under the authority of the Secretary of Defense that urgent and compelling reasons exist to promulgate the interim rule without prior opportunity for public comment. This action was necessary because of the urgent need to increase the cyber security requirements placed on DoD information in contractor systems, to mitigate the risk of compromise of covered defense information (CDI), to ensure uniform application of policies and procedures for the acquisition of cloud computing services across DoD, and to gain awareness of the full scope of cyber incidents being committed against defense contractors. The Network Penetration Reporting and Contracting for Cloud Services rule revises the Defense Federal Acquisition Regulation Supplement (DFARS) to implement section 941 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2013 (Pub. L. 112-239) and section 1632 of the NDAA for FY 2015. This rule also implements policies and procedures for use when contracting for cloud computing services.
Section 941 of the NDAA for FY 2013 requires cleared defense contractors to report penetrations of networks and information systems and allows DoD personnel access to equipment and information to assess the impact of reported penetrations. Section 1632 of the NDAA for FY 2015 requires that a contractor designated as operationally critical must report each time a cyber incident occurs on that contractor's network or information systems.

Q2: How will the Department manage the multiple versions of DFARS 252.204-7012 that currently exist?

A2: The security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Protecting Controlled Unclassified Information (CUI) in Nonfederal Information Systems and Organizations, build upon the table of NIST SP 800-53 controls contained in the November 2013 version of DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. While there is additional effort for the difference, none of the effort to implement the original controls is lost. Due to the differences in the multiple versions of 252.204-7012, however, amending the contract requires contracting officer authority and is generally bilateral, requiring contractor signature. "Block changes" and "mass mods," generally reserved for administrative changes, such as a payment office address change, are not an option for this situation. There is nothing, however, that precludes a contracting officer from considering a modification of the contract upon request of the contractor.

Q3: What is the purpose of DFARS clause 252.204-7012?

A3: DFARS clause 252.204-7012 was structured to ensure that unclassified DoD information residing on a contractor's internal information system is safeguarded from cyber incidents, and

that any consequences associated with the loss of this information are assessed and minimized via the cyber incident reporting and damage assessment processes. In addition, by providing a single DoD-wide approach to safeguarding covered contractor information systems, the clause prevents the proliferation of nonharmonized cyber security clauses and contract language by the various entities across the DoD.

Q4: When is DFARS clause 252.204-7012 required in contracts? Is the clause required in contracts for commercial items?

A4: DFARS clause 252.204-7012 is required in all solicitations and contracts, including solicitations and contracts using Federal Acquisition Regulation (FAR) part 12 procedures for the acquisition of commercial items. The clause is not required to be applied retroactively, but that does not preclude a contracting officer from modifying an existing contract to add the clause.

When the acquisition of commercial items involves CDI, such as in some cases when commercial items, services, or offerings are tailored to meet a particular customer's requirement, DFARS clause 252.204-7012 will apply to commercial items involving CDI.

Q5: When must the requirements in DFARS clause 252.204-7012 be implemented?

A5: The requirements in DFARS clause 252.204-7012 must be implemented when CDI is processed, stored, or transits, an information system that is owned by, or operated by or for, the contractor, or when performance of the contract involves operationally critical support. The contracting officer shall indicate in the solicitation/contract when performance of the contract will involve, or is expected to involve, CDI or operationally critical support. All CDI provided to the contractor by the Government will be marked when appropriate.

Q6: When and how should DFARS clause 252.204-7012 flow down to subcontractors?

A6: DFARS clause 252.204-7012 flows down to subcontractors without alteration when performance will involve operationally critical support or CDI. The contractor should consult with the contracting officer when it is uncertain if the clause should flowdown.

Flowdown is a requirement of the terms of the contract with the Government, which should be enforced by the prime contractor as a result of compliance with these terms. If a subcontractor does not agree to comply with the terms of clause 252.204-7012 then CDI should not be on that subcontractor's information system.

Q7: What are the cost recovery options for complying with DFARS clause 252.204-7012?

A7: Contractors should consult with their Audit Compliance/Accounting/Finance departments for guidance on this matter. If the contractors' Audit Compliance/Accounting/Finance departments have any questions regarding this matter they should contact their cognizant Defense Contract Management Administration and/or Defense Contract Audit Agency offices.

Q8: Will FAR clause 52.204-21, Basic Safeguarding of Covered Contractor Information Systems, and DFARS clause 252.204-7012 be used in the same solicitation/contract?

A8: Yes. The prescribed use of each of these clauses is not reliant on the inclusion of the other clause. Most solicitations/contracts that include CDI will also include non-CDI Federal contract information that requires protection in accordance with the Basic Safeguarding FAR clause. In addition, it is likely that non-CDI Federal contract information will be flowed down to a subcontractor even when CDI is not, and as such, the FAR clause will flow down as well.

Q9: Is information identified as FOUO considered to be CDI?

A9: Information that is identified as For Official Use Only (FOUO) alone does not indicate that it is CDI. Information identified as FOUO should only be treated as CDI when the information falls within the definition of CDI. Most FOUO information does not meet this requirement. For more information on FOUO markings see DoD Manual 5200.1, Vol 4.

Requiring activities/contracting officers should not identify all FOUO to contractors as CDI. However, there may be cases where the CDI provided by Requiring Activities (e.g., Privacy information) may be marked as FOUO. In such cases the requiring activity should distinguish the FOUO information requiring protection as CDI from any other FOUO marked material – this is particularly important since the protections required may differ based on the category of "FOUO" information.

Q10: Who is responsible for identifying/marking unclassified CDI? How will CDI be identified?

A10: The requiring activity is responsible to:

- Mark or otherwise identify in the contract, task order, or delivery order, information that will be provided to the contractor in connection with the performance of the contract;
- Determine if CDI is collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

The contracting officer shall ensure that identification of CDI is included in the contract, task order, or delivery order, and ensure that the contract, task order, or delivery order includes the requirement, as provided by the requiring activity (such as a contract data requirements list) for the contractor to mark CDI developed in the performance of the contract. None of the information should be marked as "covered defense information" or "CDI," but should be identified by the category of information from the CUI Registry.

Q11: What is Unclassified Controlled Technical Information (CTI)?

A11: Controlled technical information is defined in the DFARS at 204.7301 as technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.

Q12: What is "Operationally Critical Support"? How will it be identified?

A12: Operationally critical support is defined as supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation. The contract will include notification of when the contractor will provide operationally critical support.

DoD identifies three types of operationally critical support. Examples include but are not limited to the following:

(i) Operationally critical support for mobilization, which is addressed under (ii) and (iii).

(ii) Operationally critical support for distribution includes, but is not limited to:
   a. Airlift, sealift, aeromedical, and intermodal transportation services and their associated material handling and ground handling labor or stevedore services.
   b. U.S. railroad, truck, barge, ferry, and bus services provided by passenger and freight carriers and their associated material handling and ground handling labor services.
   c. Third party logistics (3PL) services provided by non-equipment owned brokers and freight-forwarders.
   d. Transportation Protection Services for arms, ammunition, and explosives (AA&E) and courier materiel.
   e. Transportation and packaging of hazardous material.
   f. Information technology systems and network providers essential to the command, control operation, and security of contingency transportation mission functions delineated in "a" through "e".

(iii) Operationally critical support for sustainment includes, but is not limited to:
   a. Local acquisition of liquid logistics (water, fuel-all types); Class 1, fresh fruits and vegetables; local meat/bread products, and bottled gases (e.g., helium, oxygen, acetylene).
   b. Supply chain for rare earth metals.
   c. Procurement and product support for critical weapons systems identified by the requiring activity.
   d. The prime contractors and subcontractors for critical weapons systems in development and sustainment that are fielded to the Area of Responsibility (AOR).
   e. Contractor Logistics (maintenance and supply) Support.
   f. Depot-level maintenance for critical items, particularly in Public-Private Partnerships.

g. Information technology systems and network providers essential to the command, control operation, and security of contingency supply and maintenance mission functions delineated in “a” through “f”.

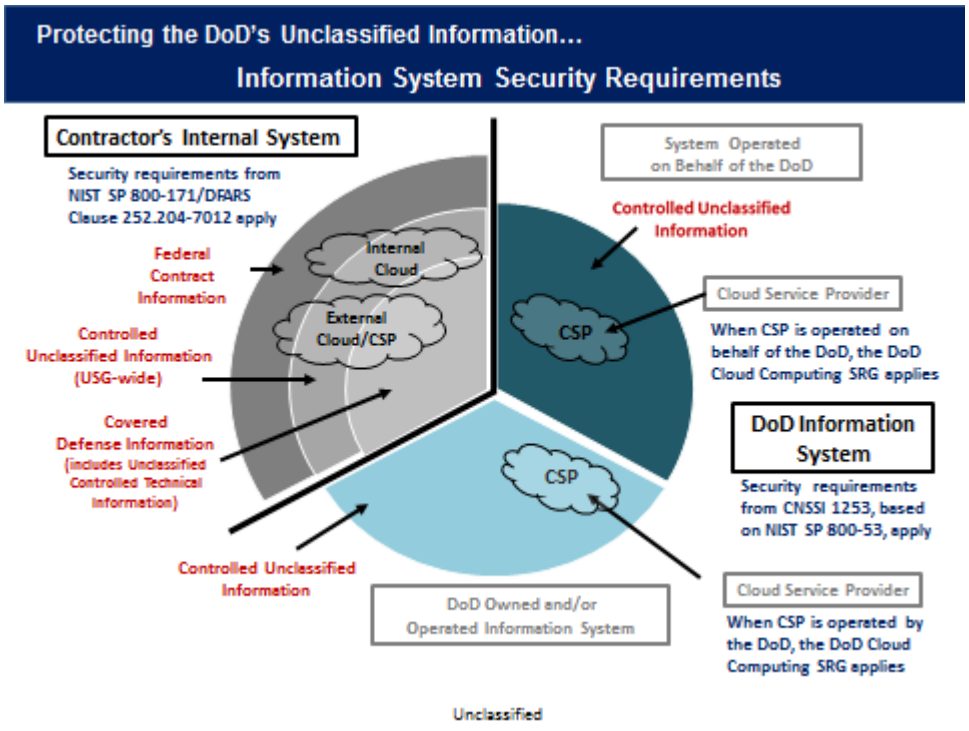
The contracting officer will be notified by the requiring activity when the contractor will provide operationally critical support. The contracting officer shall ensure that notification of operationally critical support provided is included in the contract, task order, or delivery order.

Q13. What should the Contractor do if covered defense information (CDI) or operationally critical support is not identified in the contract, task order, or delivery order, and the Contractor becomes aware that CDI or operationally critical support during performance of the contract?

A13: Contact the contracting officer.

Q14: How are the security protections required for a contractor’s internal information system different than the protections required for a DoD information system?

A14: The protections required to protect Government information are dependent on the type of information we are protecting, and on the type of system on which the information is processed or stored. The following diagram illustrates the requirements for protecting covered defense information, controlled unclassified information, and Federal contract information when processed or stored on a contractor’s internal information system, or on a DoD information system. For a more thorough description of this diagram, go to: http://www.acq.osd.mil/dpap/pdi/network_penetration_reporting_and_contracting.html



Q15: Why did the security protections required by DFARS clause 252.204-7012 change from a table of selected NIST SP 800-53 security controls to NIST Special Publication (SP) 800-171? How does NIST SP 800-171 compare to NIST SP 800-53?

A15: The change in required security protections was made for several reasons. The full set of NIST SP 800-53 security controls is intended for internal use by the Federal Government. It contains requirements that often do not apply to a contractor's internal information system, which is why the initial version of the DFARS clause 252.204-7012 included only a selected subset of those controls. In contrast, the new NIST SP 800-171 security requirements were developed specifically to be applied to, and by, nonfederal organizations. They are performance-based to avoid mandating specific solutions, and to make it easier to apply to existing systems in use by industry. The new NIST 800-171 also provides a standardized and uniform set of requirements for all CUI security needs, allowing nonfederal organizations to be in compliance with statutory and regulatory requirements, and to consistently implement safeguards for the protection of this information.

It is important to note that the contracting officer should ensure that the requiring activity describes the security requirements and assessments based on the contents of NIST SP 800-171 and its Basic and Derived Security Requirements only, and not on NIST SP 800-53 security controls, i.e., they should not reference a NIST SP 800-53 control (e.g., AC-4) in order to identify a NIST SP 800-171 security requirement (e.g., 3.1.3).

DFARS rule 2013-D018 amends the security controls required to provide "adequate security" – replacing a table of controls based on NIST SP 800-53, with security requirements found in NIST SP 800-171,. A comparison of these requirements is shown below:

NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations	**NIST SP 800-171, Protecting CUI in Nonfederal Information Systems and Organizations, Jun 15**
• Facilitates consistent and repeatable approach for selecting/specifying security controls • Uniquely Federal (i.e., primarily the responsibility of the Federal Government) • Controls address diverse set of security and privacy requirements across Federal Government/critical infrastructure	• Developed for use on contractor and other nonfederal information systems to protect CUI. • Tailored to eliminate requirements that are: - Uniquely Federal - Not related to CUI - Expected to be satisfied without specification (i.e., policy and procedure controls)
• "Build It Right" strategy provides flexible yet stable catalog of security controls to meet current information protection	• Enables contractors to comply using systems and practices they already have in place

needs and the demands of future needs based threats, requirements, and technologies	• Intent is not to require the development or acquisition of new systems to process, store, or transmit CUI
• Provides recommended security controls for information systems categorized in accordance with FIPS 199, Standards for Security Categorization of Federal Information and Information Systems • Allows organizations to tailor relevant security control baseline to align with their mission/business environment	• Provides standardized/uniform set of requirements for all CUI security needs • Allows nonfederal organizations to consistently implement safeguards for the protection of CUI (i.e., one CUI solution for all customers) • Allows contractor to implement alternative, but equally effective, security measures to satisfy every CUI security requirement

Q16: How might a small business with limited IT or cybersecurity expertise approach meeting the requirements of NIST SP 800-171.

A16: NIST SP 800-171 was written using performance-based requirements, with the intent to not require the development or acquisition of new systems to process, store, or transmit CUI, but enable contractors to comply using systems and practices they already have in place. It eliminates unnecessary specificity and includes only those security requirements necessary to provide adequate protection for the impact level of CUI (e.g., covered defense information).

Most requirements in NIST SP 800-171 are about policy, process, and configuring IT securely, while others require security-related software (such as anti-virus) or additional hardware (e.g., firewall).

For companies that were compliant with the 2013 Safeguarding of Unclassified Controlled Technical Information DFARS clause with the table of NIST SP 800-53 controls, almost all the additional NIST SP 800-171 requirements can be accomplished by policy/process changes or adjusting the configuration of existing IT. With the exception of the multifactor authentication requirement (3.5.3), no additional software or hardware is typically required.

For companies new to the requirements, a reasonable approach would be to:

- Examine each of the requirements to determine
    - Policy or process requirements
    - Policy/process requirements that require an implementation in IT (typically by either configuring the IT in a certain way or through use of specific software)
    - IT configuration requirements
    - Any additional software required
    - Any additional hardware required.

  - If unsure of what a requirement means, companies should refer to the mapping table in Appendix D to NIST SP 800-171, identify the corresponding NIST SP 800-53 control, and consult the Supplemental Guidance related to that control in NIST SP 800-53 [Note: not all aspects of a NIST SP 800-53 control requirement may have been included in NIST SP 800-171 requirement, so not all of the Supplemental Guidance may apply].
- Typically, most requirements entail determining what the company policy should be (e.g., what should be the interval between required password changes) and then configuring the IT system to implement the policy.
- Note that when the term "control" or "manage" is used, it does not necessarily imply a technical implementation – often a process or policy (with an ability to check periodically to insure the policy/process is being followed) is sufficient.
- The complexity of the company IT system may determine whether additional software or tools are required. Small systems can manually accomplish many requirements, such as configuration management or patch management, while more complex systems may require automated software tools to perform the same task.
- Based on the above, determine which of the requirements can be readily accomplished by in-house IT personnel and which require additional research in order to be accomplished by company personnel or may require outside assistance.
- Develop a plan of action and milestones to implement the requirements.

Q17: What if the contractor thinks a required security control is not applicable, or that an alternative control or protective measure will achieve equivalent protection?

A17: The rule allows for the contractor to identify situations in which a required control might not be necessary or for an alternative to a required control. In such cases, the contractor should provide a written explanation in their proposal describing the reasons why a control is not required or adequate security is provided by an alternative control and protective measure. The contracting officer will refer the proposed variance to the DoD CIO for resolution. The DoD Chief Information Officer (CIO) is responsible for ensuring consistent adjudication of proposed non-applicable or alternative security measures.

When CDI is used in performance of a subcontract, the requirement is for the subcontractor to request the contracting officer to seek CIO adjudication on variances from NIST SP 800-171 requirements.

Q18: What is the process used by the DoD CIO to adjudicate alternative/non-applicable controls?

A18: DFARS provision 252.204-7008 provides a process for the contractor to identify situations in which a security requirement from NIST SP 800-171 might not be necessary, or the contractor proposes an alternative to a security requirement from NIST SP 800-171. In such

cases, the contractor must provide a written explanation in their proposal describing the reasons why a security requirement is not applicable, or how alternative, but equally effective, security measures can compensate for the inability to satisfy a particular requirement. The contracting officer will refer the proposed variance to the DoD CIO for adjudication. The DoD Chief Information Officer (CIO) is responsible for ensuring consistent adjudication of proposed non-applicable or alternative security measures. If the DoD CIO needs additional information, a request is made to the contracting officer. The resultant DoD CIO adjudication is provided to the contracting officer, who in turn advises the contractor of the decision. The timeframe for response by the DoD CIO is typically within five business days.

Q19: What are the criteria used by the DoD CIO in adjudicating alternative/non-applicable controls?

A19: The basis for judging acceptability of an alternative is whether it is equally effective; the acceptability of "not applicable" is if the basis/condition for the requirement is absent.

Q20: How can DoD consider an offeror's compliance with NIST SP 800-171 in the source selection process?

A20: The intent of DFARS clause 252.204-7012 is to ensure that the security requirements in NIST SP 800-171 are applied to information systems that are owned by, or operated by or for contractors, and process, store, or transmit CDI. The clause is not structured to require contractor compliance with NIST SP 800-171 as a mandatory evaluation factor in the source selection process, but the requiring activity is not precluded from stating in the solicitation that it will consider compliance with NIST SP 800-171 in the source selection process. Examples of how a requiring activity might proceed include:

- Notifying the offeror that its approach to protecting covered defense information and providing adequate security in accordance with DFARS 252.204-7012 will be evaluated in the solicitation on an acceptable or unacceptable basis. Proposal instructions and corresponding evaluation specifics of what constitutes acceptable/unacceptable compliance with NIST SP 800-171 must be detailed in sections L and M of the solicitation as well as the Source Selection Plan.
- Establishing compliance with DFARS 252.204-7012 as a separate technical evaluation factor and notifying the offeror that its approach to providing adequate security will be evaluated in the source selection process. The specifics of how offeror compliance with NIST SP 800-171, will be evaluated must be detailed in Sections L and M of the solicitation as well as the Source Selection Plan.

Q21: Does the Government intend to monitor contractors to ensure implementation of the required security requirements?

A21: The DFARS rule did not add any unique or additional requirement for the Government to monitor contractor implementation on the required security requirements. Contractor compliance with these requirements would be subject to any existing generally applicable contractor compliance monitoring mechanisms.

Q22: Will the DoD certify that a contractor is 100% compliant with NIST SP 800-171? Is a 3rd Party assessment of compliance required?

A22: No new oversight paradigm is created through this rule. If oversight related to these requirements is deemed necessary, it can be accomplished through existing FAR and DFARS allowances, or an additional requirement can be added to the terms of the contract. The rule does not require "certification" of any kind, either by DoD or any other firm professing to provide compliance, assessment, or certification services for DoD or Federal contractors. Nor will DoD give any credence to 3rd party assessments or certifications – by signing the contract, the contractor agrees to comply with the terms of the contract. It is up to the contractor to determine that their systems meet the requirements.

Some companies with limited cybersecurity expertise may choose to seek outside assistance in determining how best to meet and implement the NIST SP 800-171 requirements in their company. But, once the company has implemented the requirements, there is no need to have a separate entity assess or certify that the company is compliant with NIST SP 800-171.

Q23: How does the Contractor report a cyber incident?

A23: When reporting a cyber incident under DFARS clause 252.204-7012, or under DFARS clause 252.239-7010, Cloud Computing Services, the contractor will access the DIBNet portal (http://dibnet.dod.mil) and complete the fields in the Incident Collection Format (ICF). Access to this form requires a DoD-approved medium assurance public key infrastructure (PKI) certificate. In the event a company does not have anyone with a DoD approved medium assurance certificate, they may contact the DoD Cyber Crime Center (DC3) (contact information is also on the portal) for additional information. The DIBNet portal is DoD's single reporting mechanism for DoD contractor reporting of cyber incidents on unclassified information systems. The rule streamlines the reporting processes for DoD contractors and minimizes duplicative reporting processes.

Q24: How can the contractor obtain DoD-approved medium assurance External Certificate Authority (ECA) certificate in order to report?

A24: For information on obtaining a DoD-approved ECA certificate, please visit the ECA website (http://iase.disa.mil/pki/eca/certificate.html).

Q25: What should the contractor do when they do not have all the information required by the clause within 72 hours of discovery of any cyber incident?

A25: When a cyber incident is discovered, the contractor/subcontractor should report whatever information is available to the DIBNet portal within 72 hours of discovery. When more information becomes available, the contractor/subcontractor should submit a follow-on report with the added information.

Q26: What happens when the contractor submits an ICF to the DIBNet portal?

A26: Upon receipt of the contractor submitted ICF in the DIBNet portal, the DC3 (the designated collection point for cyber incident reporting required under DFARS clause 252.204-7012) will send an unclassified email containing the submitted ICF to the contracting officer identified on the ICF. The contracting officer is directed in the DFARS Procedures, Guidance and Information (PGI) 204.7303-3 to notify the requiring activities that have contracts identified in the ICF.

Q27: What role does the DoD Cyber Crime Center (DC3) play in the DFARS reporting program?

A27: The DoD Cyber Crime Center (DC3) serves as the DoD operational focal point for receiving cyber threat and incident reporting from Defense contractors.

Q28: Why are subcontractors required to simultaneously report incidents directly to the Government and the prime contractor? Can you provide clarification regarding the types of information that must be disclosed by subcontractors to prime contractors.

A28: The rule clarifies that that subcontractors are required to rapidly report cyber incidents directly to DoD at http://dibnet.dod.mil, and to provide the incident report number, automatically assigned by DoD, to the prime contractor (or next higher-tier subcontractor) as soon as practicable. Any requirement for the subcontractor to provide anything more than the incident report number to the prime contractor (or next higher-tier subcontractor) is a matter to be addressed between the prime and the subcontractor. The DoD will protect against the unauthorized use or release of cyber incident information reported by the contractor or subcontractor in accordance with applicable statutes and regulations.

Q29: What is meant by the language at 252.204-7009 (b)(5)(i) which states, "A breach of these obligations or restrictions may subject the contractor to criminal, civil, administrative, and contractual actions in law and equity for penalties, damages, and other appropriate remedies by the United States"?

A29: The rule subjects support services contractors directly supporting Government activities related to safeguarding covered defense information (CDI) and cyber incident reporting (e.g.,

providing forensic analysis services, damages assessment services, or other services that require access to data from another contractor) to restrictions on use and disclosure obligations. The statement quoted above is found in DFARS clause 252.204-7009, "Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information." This clause limits access and use of CDI by contractors supporting DoD activities triggered by the reported cyber incident, and requires contractors to ensure that their employees are subject to use and non-disclosure obligations consistent with the clause. The clause operates as a non-disclosure agreement (NDA), authorizing DoD support contractors to access and use CDI "only for the purpose of furnishing advice or technical assistance directly to the Government in support of activities related to DFARS clause 252.204-7012" (e.g., providing support for cyber incident report analysis and damage assessment processes). That quoted language in DFARS clause 252.204-7009 is not about compliance with the security requirements required by DFARS clause 252.204-7012, but about support contractors' misuse of third party information they receive in supporting DoD cyber incident analysis and damage assessment processes.

Q30: How does the contractor submit media?

A30: The contracting officer will send instructions for submitting media when a request to submit media is made.

QUESTIONS SPECIFIC TO THE NIST SP 800-171 SECURITY REQUIREMENTS:

Q31: **How will the DoD account for the fact that compliance with NIST SP 800-171 is an iterative and ongoing process? The DFARS clause imposing NIST SP 800-171 requires that the entire system be in 100% compliance all the time, a condition that in practice (in industry or Government) is almost never the case.**

For example:

- **It is not possible to apply session lock or termination (Requirements 3.1.10/11) to certain computers (e.g., in a production line or medical life-support machines).**
- **Applying a necessary security patch can "invalidate" FIPS validated encryption (Requirement 3.13.11) since the encryption module "with the patch" has not been validated by NIST.**
- **Segments of an information system may be incapable of meeting certain requirements, such as correcting flaws/patching vulnerabilities (Requirement 3.14.1) without disrupting production/operations that may be critical to the customer.**

How should a contractor deal with situations such as these?

A31: The DFARS requirement at 252.204-7012 (b)(1)(ii)(A) to, "implement information systems security protections on all covered contractor information systems including, at a minimum, the security requirements in NIST SP 800-171," is not intended to imply there will not be situations where elements of the NIST SP 800-171 requirements cannot practically be applied, or when events result in short or long term issues that have to be addressed by assessing risk and applying mitigations. The rule allows a contractor to identify situations in which a required control might not be necessary or an alternative but equally effective control can be used, and the DoD CIO will determine whether the identified variance is permitted, in accordance with DFARS provision 252.204-7008(c)(2)(i) and (ii).

In addition, the dynamic nature of cybersecurity threats and vulnerabilities is recognized within the NIST SP 800-171. The contractor should address situations such as those listed above in accordance with the NIST SP 800-171 Requirements that follow:

- 3.11.1, Risk Assessment: Requires the contractor to periodically assess the risk associated with operating information systems processing CUI
- 3.12.1, Security Assessment: Requires the contractor to periodically assess the effectiveness of organizational information systems security controls; and
- 3.12.2, Security Assessment: Requires the contractor to "develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems."

DoD estimates that a contractor system that was compliant with the previous DFARS clause would be 90-95% compliant with the NIST 800-171 security requirements by implementing policy and procedure requirements which do not involve substantive IT changes. The contractor may then address any residual issues, e.g., security requirement implementations in progress, through "plans of action" (as described in security requirement 3.12.2 noted above) in the contractor's equivalent of a system security plan. The "system security plan" is addressed in NIST 800-171 as "expected to be routinely satisfied by nonfederal organizations without specification" as part of an overall of a risk-based information security program (see footnote 16, page 6 and Table E-12, PL-2). The system security plan should be used to describe how the system security protections are implemented, any exceptions to the requirements to accommodate issues such as those listed in the question above, and plans of action as provided by security requirement 3.12.2, to correct deficiencies and reduce or eliminate vulnerabilities.

Elements of the security plan may be included with the contractor's technical proposal (and may subsequently be incorporated as part of the contract). These also may inform a discussion of risk between the contractor and requiring activity/program office.

Q32: Do all the 171 requirements for cryptography have to be FIPS validated, and if so, what does that mean? If the algorithm is FIPS approved, is that sufficient?

A32: Yes, the requirement is to use FIPS-validated cryptography, which means the cryptographic module has to have been tested and validated to meet FIPS 140-1 or-2 requirements. Simply using an approved algorithm is not sufficient – the module (software

and/or hardware) used to implement the algorithm must be separately validated under FIPS 140. More information is available at http://csrc.nist.gov/groups/STM/cmvp/ and http://csrc.nist.gov/groups/STM/cmvp/validation.html

Q33: Must all cryptography used in a covered information system be FIPS validated?

A33: No. Requirement 3.13.8 states: "Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards." FIPS validated cryptography is required only to protect CUI and only when transmitted outside the protected environment of the covered information system if not separately protected (e.g., by a protected distribution system).

Q34: Security requirement 3.1.9 requires "privacy and security notices consistent with applicable CUI rules." Which CUI rules are being referenced?

A34: This requirement references the National Archives and Records Administration's (NARA) Federal rule (32 CFR 2002) implementing its CUI program. It would apply if a specific type of CUI (i.e., information that requires safeguarding or dissemination controls pursuant to law, regulation or Governmentwide policy) requires such notices (e.g., before accessing or entering the data).This is not common.

Q35: Security requirement 3.1.21 requires limiting the use of organizational portable storage devices on external information systems. Is this expected to be done using technical means or by policy? If there are technical options, can you provide any examples?

A35: This is generally implemented by policy, though some devices can be configured to work only when connected to a system to which they can authenticate (this is, however, not a requirement).

Q36: Security requirement 3.1.21: Can you provide a definition of "portable device", as that is not defined in NIST guidance?

A36: A 'portable storage device' (the term used by NIST) is an information system component that can be inserted into and removed from an information system, and that is used to store data or information (e.g., text, video, audio, and/or image data). Such components are typically implemented on magnetic, optical, or solid state devices (e.g., floppy disks, compact/digital video disks, flash/thumb drives, external hard disk drives, and flash memory cards/drives that contain non-volatile memory). References: NIST 800-171, Appendix B, Glossary; NIST 800-53, Appendix B, Glossary

Q37: Security requirement 3.4.9 - Control and monitor user-installed software: this requirement, and security requirement 3.13.13, Control and monitor the use of mobile code,

seem outside the scope of protecting CUI. Shouldn't the requirement be to control CUI processing to authorized software?

A37: This requirement, and the requirement for mobile code, are necessary to protect the overall system processing CUI. They are not about software used to actually process CUI.

Q38: Security requirement 3.5.3 - Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. What is meant by "multifactor authentication?"

A38: Multifactor authentication to an information system uses two or more methods of authentication involving something you know (e.g., password); something you have (e.g., a One-Time Password generating device like a fob, smart-card, or a mobile app on a smart-phone); and something you are (e.g., a biometric like a fingerprint or iris). The traditional authentication method uses a single factor, typically a password, while multifactor authentication requires that a second factor also be used such as PIN sent via a text message (using something you have – the cell phone) or something you are (fingerprint).

Q39: Can one of the factors in multifactor authentication be where you are (e.g., within a controlled access facility)?

A39: No. Multifactor requires at least two of the following three factors: what you know, what you are, and what you have. Where you are is not one of these factors.

Q40: Native 2-factor authentication support for network access on all platforms is problematic; how is the multifactor requirement met?

A40: The multifactor authentication system is a requirement for local or network access to the information system, which is different from authentication to a specific information system component (e.g., a router) or an application (e.g., database). While many system components and applications now support (and expect) multifactor authentication, it is not a requirement to implement two-factor authentication on specific devices**.**

Q41: Do I need to use "multifactor authentication" for a smartphone or tablet?

A41: If the device is used as a mechanism to access the organization's information system (e.g., via a web interface), then the information system itself must require the multifactor authentication, which would be entered by means of the mobile device. DoD does not consider e-mail or text messages "pushed" from an organization's information system as "accessing" the information system, and requiring multifactor authentication. Multifactor authentication to the device itself (e.g., to open the device) is not required as (1) no current devices appear to support more than a single factor; (2) there is a separate security requirement (3.1.19) to

encrypt any CUI on the mobile device; and (3) multifactor authentication is not required to decrypt the CUI.

Q42: What if I have CDI on my smartphone or tablet (e.g., in company e-mail) – do I need to use multifactor authentication in that case?

A42: No, that is covered under a separate security requirement, 3.1.19 - Encrypt CUI on mobile devices. As noted above, the multifactor authentication requirement applies to an information system, and a mobile device in not considered an "information system." But, if there will be CDI on a mobile device, it must be encrypted. This can be done by encrypting all the data on the device (as is typically done on a laptop, and is available with recent iOS devices and some Android/Windows devices) or via a container (like the Good app, which is available for iOS (iPhone, iPad), Android, Windows; Blackberry's Secure Work Space for iOS and Android; etc.) to separate the CDI from the other information on the phone (or company information from personal information if employing a bring your own device (BYOD) approach). Care should be taken to ensure the encryption module is FIPS-validated for either the whole device or container. Information that is independently and appropriately encrypted (e.g., an e-mail encrypted with a PKI certificate) is self-protecting and need not be double-encrypted.

Q43: If a systems administrator has already been authenticated as a normal user using multifactor authentication, does using his administrative password to install software on the system violate the multifactor requirement?

A43: A privileged user (e.g., systems administrator) should always be in the "privileged" role to administer – e.g., he should use multifactor authentication in his privileged role (not as a normal user) to logon to the system to perform administrative functions.

Q44: Security requirement 3.5.4 – The requirement to employ replay resistant authentication mechanisms for network access to privileged and non-privileged accounts. What defines replay resistant?

A44: Per NIST 800-53, "authentication processes resist replay attacks if it is impractical to achieve successful authentications by replaying previous authentication messages. Replay-resistant techniques include, for example, protocols that use nonces or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators." Reference: NIST SP 800-53, IA-2(8,9), Identification and Authentication | Network Access to Privileged Accounts - Replay Resistant, Identification and Authentication | Network Access to Non-Privileged Accounts - Replay.

Q45: Security requirement 3.5.10 – Store and transmit only encrypted representations of passwords (in Revision 1, "encrypted representations of passwords" is changed to

"cryptographically-protected password)." Is a HASH considered an "encrypted representation" of a password or a cryptographically-protected password?

A45: Yes. The Supplemental Guidance in NIST SP 800-53 for the related security control IA-5(1) notes that "Encrypted representations of passwords include, for example, encrypted versions of passwords and one-way cryptographic hashes of passwords." Best practice would add a unique "salt" to the password before hashing.

Q46: Security requirement 3.7.5 – Can the requirement for multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete be met using other authentication and access control combinations such as remote IP address restrictions, session monitoring, and "One-Time-Pads"?

A46: The multifactor authentication for non-local maintenance is intended for recurring non-local maintenance by organizational personnel rather than episodic non-local maintenance by outside vendors where issuance of such credentials for one-time activities is not efficient and may not be advisable. Nevertheless, presuming the individual performing the repair is known and trusted, it is possible to provide for "one-time" multifactor authentication through the use of a password and a separately provided token (e.g., PIN via text message to a cell phone).

Q47: Security requirement 3.8.2 –Can digital rights management protections or discretionary access control lists meet the intent of the requirement to "limit access to CUI on information system media to authorized users?"

A47: This requirement is meant to be applied by using physical controls to access physical media, but other mechanisms for logical access, such as those mentioned, are acceptable.

Q48: Security requirement 3.8.4 – Mark media with necessary CUI markings and distribution limitations. Is this for all media, to include cell phones, for example, or just for removable media?

A48: This applies to information system media, which includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. It would not include cell phones.

Q49: Security requirement 3.10.6: Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites). Is this expected to be done using technical means or by policy? If there are technical options, can you provide any examples?

A49: This simply means that if you have alternate work sites that will be used to store, process or transmit CDI, that the same requirements apply (i.e., there is no difference in requirements

between the primary and alternate work sites), although different methods may be used to meet the requirements at the alternate site.

Q50: Security requirement 3.13.6 – The requirement to "deny network communications traffic by default and allow network communications traffic by exception" (i.e., deny all, permit by exception) is unrealistic if it must be implemented on all systems that host or transit CUI information. Can this requirement be met if there is a mechanism to implement "deny all, permit by exception" rule within the path between the external network and the CUI information?

A50: Yes, but if there are internal elements/segments of the information system that do not have the protections in place to process/store CUI, then they would also fall under this provision.

Q51: Security requirement 3.13.14. The description for the security requirement in Section 3 (3.13.14) "control and monitor the use of Voice over Internet Protocol (VoIP) technologies" is different from the corresponding Appendix D entry, "Establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies and monitor/control use of VoIP." Which is correct? How should this be handled for 3rd party VoIP service offerings where control is outsourced. (i.e., Vonage)? Does this security requirement only apply when the VoIP service is shared on a network that transits CUI?

A51: Section 3 is correct, and this has been corrected in the current posted version of NIST SP 800-171 (see Errata on page ix). Even if outsourced, the internal IT system should have protections in place to control (albeit limited) and monitor VoIP within the system. If physically or cryptographically isolated from an information system processing CUI, this control would not apply (but it would be prudent to apply the requirement).

Q52: **Regarding security requirement 3.13.14– how is CUI to be protected when transmitted over Plain Old Telephone Service (POTS)?**

A52: POTS would not normally be considered part of the information system processing CUI. Protection of CUI over the telephone is not addressed by NIST SP 800-171 or by DFARS clause 252.204-7012.

CLOUD COMPUTING

Q53: What security requirements apply when using a cloud solution to process/store Covered Defense Information?

A53: In accordance with the Federal Information Security Management Act (FISMA), when an information system is being operated on the DoD's behalf, it is considered a DoD system and so

needs to meet the same requirements as if it were operated by DoD. Accordingly, the DoD Cloud Computing Security Requirements Guide (SRG) applies when—

- A cloud solution is being used to process data on the DoD's behalf;
- DoD is contracting with a cloud service provider to host and process our data in a cloud; or
- A cloud solution is being used for processing that we (the DoD) would normally do ourselves but have decided to outsource.

NIST SP 800-171 is designed to be used by nonfederal organizations to protect CUI. Accordingly, the NIST SP 800-171 applies when:

- A contractor uses an internal cloud to do his own processing related to meeting a DoD contract requirement to develop/deliver a product, i.e., as part of the solution for his internal contractor system. (Example - contractor is developing the next generation tanker, and uses his cloud (not an external cloud service provider) for the engineering design.)